Docket No.: 20162-00547-US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Letters Patent of:
Shiho Moriai et al.

Patent No.: 7,187,769

Issued: March 6, 2007

For: METHOD AND APPARATUS FOR EVALUATING THE STRENGTH OF AN ENCRYPTION

REQUEST FOR CERTIFICATE OF CORRECTION DUE TO PTO ERROR
PURSUANT TO 37 CFR 1.322 (a) (1)

Attention: Certificate of Correction Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Upon reviewing the above-identified patent, Patentee noted a typographical error which should be corrected.

In the Bibliographic data printed on the face of the issued patent:

Block [73] "Assignee" inadvertently lists "Nippon Telegraph and Telephone **Public** Corporation". The correct assignee name is "Nippon Telegraph and Telephone Corporation".

Please correct Block [73] to read:

"[73] Assignee: Nippon Telegraph and Telephone Corporation (JP)"

The error was not in the application as filed by applicant or as prosecuted. Support for applicants' assertion of PTO error may be found in the accompanying copy of the Issue Fee Transmittal and in the copy of the USPTO's EPAS assignment information which show the correct assignee name. Accordingly no fee is required.

Transmitted herewith is a proposed Certificate of Correction effecting such amendment. Patentee respectfully solicits the granting of the requested Certificate of Correction.

Applicant believes no fee is due with this request. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 20162-00547-US from which the undersigned is authorized to draw.

Dated: April 24, 2007

Respectfully submitted,

Electronic signature: /Larry J. Hume/
Larry J. Hume
Registration No.: 44,163
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant

Attachments: Certificate of Correction
Copy of Issue Fee Transmittal (PTOL-85)
Copy of USPTO EPAS Assignment Information
Copy of front page of US 7,187,769

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

30678 7590 11/07/2006

CONNOLLY BOVE LODGE & HUTZ LLP
P.O. BOX 2207
WILMINGTON, DE 19899-2207

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/463,907	02/02/2000	SHIHO MORIAI	20162-00547-US	6943

TITLE OF INVENTION: MTHEOD AND APPARATUS FOR EVALUATING THE STRENGTH OF AN ENCRYPTION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1400	$0	$0	$1400	02/07/2007

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAFORGIA, CHRISTIAN A	2131	380-001000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Connolly Bove Lodge & Hutz, LLP
2 Larry J. Hume
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Nippon Telegraph and Telephone Corporation

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Japan

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☒ Advance Order - # of Copies 2

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 220185 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature Larry J. Hume Date 1/30/07

Typed or printed name Larry J. Hume Registration No. 44,163

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

09/463,907	METHOD AND APPARATUS FOR EVALUATING THE STRENGTH OF AN ENCRYPTION	04-24-2007::14:15:39

Patent Assignment Abstract of Title

Total Assignments: 1

Application #: 09463907 **Filing Dt:** 02/02/2000 **Patent #:** 7187769 **Issue Dt:** 03/06/2007

PCT #: NONE **Publication #:** NONE **Pub Dt:**

Inventors: SHIHO MORIAI, KAZUMARO AOKI, MASAYUKI KANDA, YOUICHI TAKASHIMA, KAZUO OHTA

Title: METHOD AND APPARATUS FOR EVALUATING THE STRENGTH OF AN ENCRYPTION

Assignment: 1

Reel/Frame: 010634 / 0179 **Received:** 03/29/2000 **Recorded:** 02/02/2000 **Mailed:** 05/18/2000 **Pages:** 2

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors: MORIAI, SHIHO **Exec Dt:** 01/18/2000

AOKI, KAZUMARO **Exec Dt:** 01/18/2000

KANDA, MSAYUKI **Exec Dt:** 01/18/2000

TAKASHIMA, YOUICHI **Exec Dt:** 01/18/2000

OHTA, KAZUO **Exec Dt:** 01/18/2000

Assignee: NIPPON TELEGRAPH AND TELEPHONE CORPORATION
19-2, NISHI-SHINJUKU 3-CHOME
SHINJUKU-KU, TOKYO 163-8019, JAPAN

Correspondent: POLLACK, VANDE SANDE & AMERNICK
EDWARD G. FAETH
SUITE 800
1990 M STREET, N.W.
WASHINGTON, D.C. 20036-3425

Search Results as of: 04/24/2007 14:15:19 PM

Disclaimer:
Assignment information on the assignment database reflects assignment documents that have been actually recorded. If the assignment for a patent was not recorded, the name of the assignee on the patent application publication or patent may be different.
If you have any comments or questions concerning the data displayed, contact OPR / Assignments at 571-272-3350

Close Window

US007187769B1

(12) **United States Patent**
Moriai et al.

(10) **Patent No.: US 7,187,769 B1**
(45) **Date of Patent: Mar. 6, 2007**

(54) **METHOD AND APPARATUS FOR EVALUATING THE STRENGTH OF AN ENCRYPTION**

(75) Inventors: **Shiho Moriai**, Yokohama (JP); **Kazumaro Aoki**, Yokohama (JP); **Masayuki Kanda**, Yokohama (JP); **Youichi Takashima**, Yokohama (JP); **Kazuo Ohta**, Zushi (JP)

(73) Assignee: **Nippon Telegraph and Telephone Public Corporation** (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/463,907**

(22) PCT Filed: **Jun. 1, 1999**

(86) PCT No.: **PCT/JP99/02924**

§ 371 (c)(1),
(2), (4) Date: **Feb. 2, 2000**

(87) PCT Pub. No.: **WO99/63706**

PCT Pub. Date: **Dec. 9, 1999**

(30) **Foreign Application Priority Data**

Jun. 2, 1998 (JP) 10-153066

(51) **Int. Cl.**
H04K 3/00 (2006.01)

(52) **U.S. Cl.** **380/1**

(58) **Field of Classification Search** 380/28, 380/29, 37, 1

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,511,123 A * 4/1996 Adams 380/29
5,623,548 A * 4/1997 Akiyama et al. 380/28
5,745,577 A * 4/1998 Leech 380/28
5,796,837 A * 8/1998 Kim et al. 380/28
5,825,886 A * 10/1998 Adams et al. 380/28
6,031,911 A * 2/2000 Adams et al. 380/29
6,035,042 A * 3/2000 Mittenthal 380/37

(Continued)

FOREIGN PATENT DOCUMENTS

JP 11-212452 * 1/1998

OTHER PUBLICATIONS

Lars R. Kundsen. Block Cipher—Analysis, Design and Application. Jul. 1, 1994. p. 53-143.*

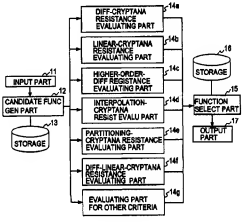
(Continued)

Primary Examiner—Christopher Revak
Assistant Examiner—Christian LaForgia
(74) *Attorney, Agent, or Firm*—Connolly Bove Lodge & Hutz, LLP; Larry J. Hume

(57) **ABSTRACT**

In the evaluation of the randomness of an S-box, measures of resistance to higher order cryptanalysis, interpolation cryptanalysis, partitioning cryptanalysis and differential-linear cryptanalysis and necessary conditions for those measures to have resistance to each cryptanalysis are set, then for functions as candidates for the S-box, it is evaluated whether one or all of the conditions are satisfied, and those of the candidate functions for which one or all of the conditions are satisfied are selected as required. It is also possible to further evaluate the resistance of such selected functions to at least one of differential cryptanalysis and linear cryptanalysis and select those of the candidate functions which are resistant to at least one of the cryptanalyses as required.

15 Claims, 2 Drawing Sheets



UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO.	:	7,187,769
APPLICATION NO.	:	09/463,907
ISSUE DATE	:	March 6, 2007
INVENTOR(S)	:	Shiho Moriai et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Correct block [73] of the patent to read:

[73] Nippon Telegraph and Telephone Corporation (JP)

MAILING ADDRESS OF SENDER (Please do not use customer number below):
Larry J. Hume
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036